An Evaluation of Optical Security Features in ID Documents, Currency and Stamps

John W. Mercer

Passport Services, U.S. State Department, Washington D.C. 20522

ABSTRACT

Optical security features have been increasingly used to protect and ensure the integrity of value documents. The types of optical features and their purposes are discussed. The application of these optical features to ID documents, currency and postage stamps are discussed. Particular attention is paid to the fraud and counterfeit resistance of the features in relation to the specific document.

Keywords: Optically variable ink, holograms, watermarks, passport, visa, ID cards, currency, postage stamps

1. INTRODUCTION

Value documents, that is documents of worth, have been around since the dawn of civilization. The seal of the king is mentioned in the Old Testament, interestingly enough in connection with two powerful women, Jezebel and Queen Esther.[1] Personal identification could be said to date even earlier, as Cain was supposedly given a special mark as punishment for the murder of his brother. But the scope of this survey paper is not to go back so far as that.

Let's push the time line forward to the 1200-1300 AD when the first watermark was developed in Italy,[2] and the first paper currency was developed in China. Even then they were concerned with counterfeiting, as the inscription on the reverse of the note prescribes death for anyone who counterfeits the notes. Of course the earliest coins date to the beginnings of civilization, but the subject of this paper is paper, not coins or the history of coinage.

Stamps as evidence of payment of proper tariffs and duties date back many centuries. One of the significant historical events leading to the revolution of the British colonies in America is commonly known as the "Stamp Act" that levied a tax on merchandise supplied to the colonies. Postage stamps are relative new comers to the security document arena. Values were usually low, a penny or five, but in those days a penny went further than it does now. Even so there was concern about counterfeiting and special features appropriate to the technology of the day, such as grilled paper or special perforations were used to identify genuine items.

As a parenthetical note it occurs to me as I write these words that the origins of each of these three classes of documents lies with the need of the government to conduct business. Kings and governments have to rule their kingdoms and countries. Official proclamations and laws have to be recognized as such. Money has to have the confidence of the people. Even stamps, which are at the basis a sales receipt for services to be rendered, need to be properly verified.

By extension, these historical happenings could be identified as the beginnings of the brand protection business, with the government's brand being on the laws, identification of its people and their mechanism for conducting business in a post-barter economy. What has happened is that the historical needs have been met with the technology available of the age. In the last twenty years the technology has been developed to add greatly to the array of features available to the document issuer. These same technologies have immediate and commercially more rewarding applications to the brand protection business. Unfortunately the commercialization of these technologies has made them available for counterfeiters,

Optical Security and Counterfeit Deterrence Techniques IV, Rudolf L. van Renesse, Editor, Proceedings of SPIE Vol. 4677 (2002) © 2002 SPIE · 0277-786X/02/$15.00

smugglers, and perpetrators of fraud--the very people these technologies are supposed to thwart. This is not unlike having the weapons taken to war being captured and turned against their original owners.

One final thing needs to be said in this introduction, namely that the words and opinions expressed in this paper belong to the author, and do not represent any official position of the US State Department or the United States government. That said, let's proceed with the evaluation of optical security features in ID documents, currency and stamps.

2. SECURITY FEATURES

Optical security features can be discussed a number of ways. I will group these security features according how they were incorporated into the particular document, that is whether they are paper/substrate-based, ink-based, optically variable devices including diffraction gratings, holograms and volume holograms or as a result of personalization printing.

2.1 Substrate-based features

Substrate-based features have two advantages, in that if the substrate is of a controlled variety, then it makes high quality counterfeiting that much more difficult. If something is in the paper, it is in there for good. Also, from a user-friendly view, security already built into the document does not have to be added on by the issuer, in the case of personalized documents.

Watermarks, mentioned above, have been around for centuries. Over time watermarks have evolved from the simple light designs one step removed from the laid lines on a deckle to sophisticated and complex portraits and designs using a large range of light and shadow. Watermarks are difficult to reoriginate, don't scan well, and personnel can easily be trained to examine watermarks. Watermarks range in price from the relatively less expensive fourdrinier dandy roller watermark consisting of a running or overall design, to the small highly detailed individual cylinder-mould watermark, to which all other printing and binding operations must be registered.

An interesting variation on traditional watermarks has been developed in Canada in recent years. Dubbed "Luminus," the substrate is a plastic sheet bonded on both sides with layers of paper, so that the finished product has the handle and printability of a good grade of paper. Any design on the core layer will show when viewed in transmitted light, so that colored watermarks are possible.

Embedded threads have been produced for several decades, primarily on cylinder mould paper machines. Threads in this use are usually narrow ribbons of coated plastic film. In the past fifteen years or so the embedded thread has become a multi-colored sophisticated carrier of information as well as an important design feature. Thread features are easy to teach, difficult to reproduce and can even be machine readable.

Planchettes are small colored disks of paper or plastic on the order of 1mm in diameter that are used to identify certain security papers. Planchettes have been used for decades. The US began putting optically variable planchettes into the data page of its passports in 1994 as a deterrent to color copying or scanning. Plastic particles in paper stock are usually called "impurities," so that paper makers do not encourage the use of plastic planchettes.

Plastic cards can have various see-through or other optical properties available in completely plastic substrates. The newest version of the INS Employment Authorization Document has variable UV properties in the core plastic layer.

2.2 Ink-based features

Ink-based features share most of the advantages of substrates, in that inks of controlled varieties are difficult to imitate, and inks provide images that may be printed in ways that are difficult to imitate, but require no further work on the part of the issuing entity, Optically variable ink (OVI®) has become an almost expected feature of any new document design. In a true OVI®, there will be a definite color change from one color to another depending on the viewing angle. The EU visa illustrates this phenomenon nicely. One characteristic of OVI® is that it requires either intaglio or silk screen printing in order to get the necessary film thickness. OVI® images are easy to train inspection personnel on, and are reliable indicators of authenticity of the printing.

Metallic inks offer copy protection, as they do not copy in true color. In addition to being out of the color gamut, the reflective surface returns too much light to the detector. In the extreme, copying a mirror creates a completely black image. Metallic inks are available from art stores and do not offer much deterrence to the counterfeiter.

Intaglio printing is the classic security print method. The ink images have a tactile feel and third-dimensional character that is not successfully imitated. This appearance is a combination of the depth of the engraved image, the highly viscous inks, and the high pressures at the printing nip.

Latent images are a special application of intaglio printing whereby two images are generated with one printing. When viewed normally, one image is seen. When the same image is viewed at a glance angle, an entirely different image is seen. Further, if this image is rotated 90 degrees in the viewing plane, the light and dark areas of the latent image swap places. The latent image is not scannable by normal copying engines and is a very reliable indicator of document authenticity.

Three are a number of other security effects that can be generated by inks. These include photochromic inks, in which an invisible ink will darken with exposure to light; thermochromic inks, which will change color on exposure to heat, usually the heat of human touch; and the various types of UV ink that glow a certain color when illuminated by UV light. With the possible exception of the thermochromic inks, none of these inks would be considered first line indicators, in that simple inspection would not see differences between false and genuine documents.

Metameric inks are inks that appear the same under regular light, but appear to be different when seen under alternate illumination. A common example of this is how a blue or red suitcase or car appears purple under mercury vapor airport lighting. Metamerism is a subtle anti-copying device that may or may not work depending on the color temperature of the scanner.

2.3 Personalization printing

In former times an ID document would have a photo attached or perhaps laminated in place. These analog photos proved to be less secure as fraudsters learned how to substitute one photo for the original. ID certification authorities resorted to alternate means of card production, special seals, card crimping and other mechanical means of making it difficult to copy the genuine method of card manufacture.

With the advent of more powerful computers and the ability to digitally print portraits, the game has changed for both the ID document issuers and for the counterfeiters and fraud community as well. Once the image is digitized, the possible output is limited only by the type of output device and the document format.

This personalization discussion primarily concerns ID and travel documents. To my knowledge currency has not been personalized. However there has been some experimentation with personalized stamps in Australia.

Laser etch cards are plastic cards in which the data has been burnt into the inner layers of the card. This requires a careful match of the materials and the laser so that the desired effect is achieved. The intensity of the laser can be adjusted so that the surface can be burnt if desired. A special case of the laser etch method is the flip image. A special linear lenticular panel on the card is engraved with a different image at two different angles, so that flipping the card between the view angles will cause the images to alternately appear and disappear.

Digital encoding of the photo can be accomplished by either of several ways. A secondary visual image can be added by systematically altering one or more of the colors so that when viewed with a flat plastic lens, the corresponding personal data, such as name or birth date, could be seen hidden in the digital printing of the person's picture. Either Jura or Graphic Security provides this capability, commonly known by the Graphic Security trade name of Scrambled Indicia. This method ties the portrait to the data in a visual way.

Digimarc Products make the second digital encoding method, and it works by manipulating individual pixels by some amount that is not visible to the eye. However scanning the image and applying the decoding algorithm will reveal the encoding. Neither method is at present a method that would by used much in primary inspection at a border, but both methods would be useful in secondary.

The most spectacular use of the digitized image is a process called Imageperf, by IAI, in which the person's photo is perforated by laser adjacent to the regular portrait. This is a very powerful tool that is already in use in Belgium and the Netherlands.

Other secondary uses of the digitized image are to print "ghost" photos next to the regular portrait. Examples of this include the UV portraits of the holders printed beside the normal portraits, as on the Japanese and the new New Zealand passports, or by printing a second smaller and less intense photo somewhere else on the data page, such as the new Czech Republic passport.

2.4 Optically variable identification devices (OVIDS)

This is a class of security measures in search of a decent generic name. Some call them holograms although quite a few have only minimal holographic activity and very few are actually made from three-dimensional models. I will not delve into the fine structure to differentiate between origination method or whether pixels are etched or whether an electron beam or laser is used to cut the master. I am more concerned about how the devices are used in the documents.

Reflective OVIDs have been used in several locations in ID documents, currency and stamps. For ID documents the reflective OVID often is applied to cover part of the portrait of the holder. This is similar to the use of reflective holograms in brand protection where the integrity of the hologram image ensures. For currency, there is no photo to protect so that the OVID serves more to authenticate the note as valid. The assumption made there is that counterfeiters will not have the tools or ability to regenerate a diffractive optical image. This is probably not a valid assumption, particularly in the cases of state-sponsored counterfeiting where the entire resources of a nation can be brought to bear.

The reflection of the OVID can arise from full or partial metallization, or other type of mechanism. The classic Kinegram® is an example of the former; the device on the present generation of Canadian currency is an example of the latter.

For ID documents, there is a danger in the use of an attention-getting shiny device, if there is not some interaction with either the personal data or the portrait. What happens is that the attention of the inspector can be drawn to the shiny character of the OVID and less attention can be paid to the rest of the document? Thus an otherwise effective OVID can actually abet fraud if the inspection is not rigorous.

Transparent OVIDs are of two general designs: localized, and overall. These could also be called "spot" and "wallpaper." An excellent example of the localized format is the new UK passport, which bears a highly active holographic patch over the digital portrait. Overall transparent OVID patterns can be either registered to the print image and the document, or just a repeating optically active pattern. The newest US passport is an example of the former, the BCC card an example of the latter.

Overall or wide-area holograms are gaining in popularity as important design elements, particularly when used as membrane-thin transfer films as carriers for personalization printing. For laser toner print which has little tendency to penetrate the substrate, a frangible film incorporating an OVID is virtually mandatory.

For ink jet personalization, the frangible holographic film adds a measure of protection for the printing, and an extra layer of easily identified security.

This discussion of protective films prompts the following observation: The day of the thick laminate should be over. How thick is thick? If the film, usually polyester, can be peeled off the document intact, then the film is too thick. Even a one mil (0.025 mm) polyester film is too thick—recall that this film is used in cassette tape for its stability and strength! The ability to lift or separate these films intact from the portrait of data underneath their "protection" allows easy access, and after the alteration, the restored, undamaged film serves to cover up the fraud that has occurred.

Design of the optical image is very important, particularly for transparent OVIDs. Enough activity should cross over and interact with the portrait and data so that tampering would be evident, but that the data should not be obscured. Many document inspections take place in less than perfect lighting situations, such as someplace along a lonely border, in a bar, or even in a poor lit airport terminal. The data has to be legible under these conditions. The other extreme is not good either, as too much optical busyness can detract from the legibility of the document.

Volume holograms have been around for many years. They are of intermediate transparency: less than the transparent thin films, but certainly more transparent than a metallized, reflective OVID. In my opinion, they have operated in the shadow of the reflective, diffractive grating type of hologram. This fall, volume holograms took a giant step into visibility as the German government has adopted volume holograms as the most visible upgrade to their passport data page and national ID card. In their application, the portrait of the holder, already shown in photographic detail, is replicated as a volume holographic image adjacent to the regular portrait.

3. WHAT ARE THE SECURITY FEATURES GOOD FOR?

In the previous decade or so the industry has shown that they can put a hologram or optical device on almost any product, from security document to CDs, license plates, blue jeans and probably even fresh fruit. My question becomes "What is the purpose of the optical feature?" Does the feature or device function as a validator for the document, like a credit card hologram, or does it actually help the document function and protect it from fraud and other creative misuse, like the transparent overlays I mentioned before. Can the optical feature be machine read, at speeds appropriate to the document? Are there any other benefits from the optical feature, or have the features been included as a technical tour de force, just because they were available and the document printer could do the device?

To address these questions, the specific types of documents have to be examined and an analysis done of what role the optical security features can fill for each type of document. This is not an easy task to do because each document is not made in a vacuum, but is the result of a complex mix of interests. To examine one passport certainly is not to be able to generalize to all.

3.1 ID documents

The purpose of identity documents is to identify the person and to define their relation to some association or thing. This may be a school ID, a video club membership, a medical card, a green card, a driver's license or a passport. In many cases the ID has a photo of the intended holder. However many identity cards do not need a photo to function, such as a library card or gas station fast pass. In fact one of the most important identity documents almost never has a photo attached to it. The document is the birth certificate, certified copies of which are one of the primary pieces of evidence of citizenship used when applying for a passport. Even though each parent might claim differently, the truth of the matter is that most babies look like, well, other babies. Photos in that case wouldn't do much good.

So let's consider the features of several representatives of each of the types of documents.

3.1.1 German ID card

The German "Personalausweiskarte" began to be issued in 1987 and by now more than 112 million have been issued. Although the quality of the card and its security features have kept fraud very low, newer technologies for scanning and reproduction have become available, so that it was time to raise the security bar once again.

In the fall of 2001, Germany began to issue a revised version of the ID-2 sized card. While keeping many of the features of the previous card, a number of special security features have been added to the face of the card. The most striking is the addition of a volume hologram reproduction of the portrait of the holder adjacent to the normal portrait that is visible when lit with UV light. Other UV visible features include Kinematic® structures over the portrait, a German eagle superimposed over the visible eagle, and the entire machine readable zone reproduced in UV immediately above the visible MRZ data.

In all cases, the visible text data interacts with the UV images or with the other physical and tactile features in the laminate of the card, so that it is almost impossible to even contemplate making a successful fraudulent alteration of the document. The same technology and features are being added to the German passport.

3.1.2 Swiss ID card

The Swiss ID card dates to about 1995-1996 time frame. It is an ID-1 sized document, manufactured by Trub. The polycarbonate card is personalized by the laser etch process. On the front of the card is a very active Kinegram® image of a hexagonal crystal with the letters CH included. The card number is etched through the Kinegram®. On the reverse is a lenticular image through which the year of expiry and the document number are etched. Other security features are evident, such as split-fountain printing and microprinting.

This was one of the first polycarbonate cards. In addition to long life, the cards make a distinctive metallic plinking sound when dropped on a hard surface. The reverse of the card contains the standard three line OCR-B machine readable zone for use as a travel document.

3.1.3 Driver's license

The generic US state driver's license is an ID-1 size card. On the face of the card is the portrait of the holder, along with their personal information. The artwork is specific to the state, as are other details, like portrait background color and whether the portrait is face-on, profile or three-quarter view. Almost all licenses have some type of optical variable effect on the front, whether it is a metallic ink or a patch of a color shifting material like the Advantage® material. The choice of the optical feature often depends on which vendor gets the contact. This competition is good for the competitive system, but it is not so good for consistency of appearance and for fraud detection.

The reverse of the driver's license is at this point very much the choice of the state. For instance, the 1999 model of the Virginia driver's license contains both a one-D and a two-D bar code.

There is movement to standardize the characteristics of driver's licenses. This was well in progress before the World Trade Center suicide attacks, but the disaster has focussed attention to the physical and operational characteristics of the driver's license. The International Standards Organization (ISO) Joint Testing Committee 1 (JTC1), Subcommittee 17 (SC17) on ID Cards and Related Media have recently formed a Working Group (WG10) on international driver's licenses. Within the United States, the American Association of Motor Vehicle Administrators (AAMVA) has been working to develop standards for driver's licenses for sever years.

The United States has no national ID card, and there is strong negative feeling toward the idea of such a card. The Driver's license is one of the principal documents that fill the niche that would be occupied by the national ID card, if there ever were to be such an item. The Social Security Card, although it has had security features added to it, is not an ID card in any real sense, and the US passport, while greatly improved, is carried by less than twenty percent of Americans.

3.1.4 Passport

Passports are long term, multi-use documents. Most passports are good for five or ten years. Passports are expected to be durable in circulation and that means that the document security features have to remain alive and effective for that term, as well. Recent work of the joint International Civil Aviation Organization (ICAO) and ISO working groups on Minimum Security Standards for Travel Documents has produced a proposed Standard for document security features, which will be placed before the ICAO Technical Advisory Group (TAG) for Machine readable travel documents in February, 2002.

Let me use as an example the document I know best, the US passport. The most recent version of the US passport debuted in November 1998, and over the next thirty-seven months has been deployed to all sixteen domestic US passport agencies. Passport production has run a little more than seven million a year for the last two years. It conforms to the ICAO Standard for machine readable passports in almost all respects.

To date, there have been no very deceptive frauds detected against the document. There have been a few attempts but they have been easily detected by the INS inspectors or others whose job it is to examine passports. One reason for this success has been that there is still an adequate supply of the photo-bearing passport that is much more susceptible to photo-substitution than the new version.

We believe the reasons for this success lies in the elimination of the hard-copy photo as a target of choice for fraud, and the optical holographic design that covers all major data points. This design or more properly set of design elements is contained in a microns-thin transparent layer that covers the whole passport data page. The finished product has an appearance that says, "This is the real thing!" Alterations to the data show up clearly to even rookie inspectors.

Of course there are many new passports that have been developed in the last two to three years. Both France and Belgium, long holdouts for the non-MRP, have developed very impressive new MRPs with complex optical features including perforated secondary photos and multi-layer break-away Fasver membrane laminate films. Portugal's new passport is very nice, as is the newest UK passport, with a holographic laminate patch protecting the portrait. Singapore and Malaysia both have relatively new passports. The Singapore book employs a mix of novel new reflective optical features, while the Malaysian book boasts a contactless chip embedded in the cover. Hardly optical, but impressive nonetheless. The second printing of the holders portrait in a different size or medium is shown by the reduces size visible ghost face on the Czech Republic passport, and the UV face being used on the new New Zealand passport and on the revised Japanese passport.

Do all these features guarantee success? No, of course not. Not even all of them on the same document would guarantee success against a determined forger or counterfeiter. Besides which all of the features together would fight among themselves and be so confusing that the document would probably be less strong against fraud.

3.1.5 Visas

The US machine readable visa is one of the few visas that have the portrait of the holder printed on the visa label. Unfortunately the combination of laser toner printing on a non-absorbent plastic substrate has been shown numerous times in all shady parts of the world to be very vulnerable to data erasure. The UV printing has had some success in reducing data alteration, but the fraudsters have learned techniques that allow them to alter the data without altering the UV print feature. The little patch of OVI® ink in the intaglio heading then serves to validate an altered visa. Not good.

To alleviate this situation, we are changing to an ink jet print method on paper that will be more absorbent and allow more anti-forgery substances to be in the substrate. We have also added other print features, and added what we believe is the first latent image and OVI® ink combination.

The EU or Schengen visa has been for a long time one of the best quality visas. The Kinegram® is stamped onto the paper after offset printing but before the intaglio, so that the Kinegram® is itself protected by being interlaced with the other print features. However the Schengen visa does not use the portrait of the holder. This is about to change. Stay tuned for the final results.

3.2 Currency

Currency is a multi-use, non-personalized medium of exchange. The biggest threat to currency is counterfeiting. In former times counterfeiting required plates and knowledge of printing. Consequently the best counterfeit deterrents were those that involved design details that a careless printer would miss. Times have changed. The high quality scanners don't usually miss design details, and ink jet printing has become the print method of choice, so prior skill is no longer required. So the problem becomes to identify what features will be effective in circulation, that can be produced by the security printer or their suppliers. Ability to withstand abuse in circulation is also a must, as currency gets much less respect from its holders than does the average passport or visa. And the best fraud deterrent features are the most obvious ones that can be used by a cashier or any person on the street.

There are two books that are excellent references: The Moneymakers, by Willibald Kranister,[3] and The Brotherhood of Money, by Murray Bloom.[4] Both books unfortunately are dated and there is a need for a more recent book with updated technology.

I always start these discussions with the paper. Special papers for currency have been used for centuries. The advent of thread inclusions, and then windowed thread from the great European papermakers has added greatly to fraud deterrence. Demetallized and multi-colored plastic threads have been worthwhile additions. Interestingly enough, one of the oldest paper features, the watermark, has continues to be a highly effective deterrent feature, even in the times of the scanner and other means of reproduction.

Inks have likewise increased in sophistication. Offset inks can have all manner of interesting properties, and offset and intaglio combination prints are becoming the norm, where once intaglio only was sufficient. The most important intaglio ink development in the last twenty years has been the invention of Optically Variable Ink (OVI®) by SICPA. First used on the Thai 60 baht note in the late 1980s OVI has come to be expected on any note design. No matter how good the scanner, the output of the printer is not going to show the optical activity of the OVI® pigment. The popularity of OVI® has even sparked an increased use of silk-screen presses for security printing. Once limited to T-shirts and banners, many printers have had to expand into silk-screen to provide increased capability.

Foil stamped devices such as the Kinegram® have been used on currency since 1988 when the 5000 Austrian schilling note debuted.[5] Since then many other notes have adopted the Kinegram.® The new series of Euro notes seemed to face a controversy as to choice of optical feature, Kinegram® or OVI®. In a classic resolution, a compromise was struck, and both will appear on the Euro notes.

Some currencies have used perforations to denominate, and the effect is quite striking.

An argument could be made that the synthetic substrate now being used for certain currencies is an optical device, but I don't agree. Certainly the localized transparent properties facilitate the use of a hologram, but the substrate itself is not an optical element.

3.3 Postage Stamps

Postage stamps have been described as miniature works of art, or evocative of the nation's history or in other grand terms. I should like to suggest that a postage stamp is a very attractive sales receipt, a single-use, non-personalized (in most cases) sales receipt. Of course one does not go to the counter and ask for a packet of receipts. We often ask for certain designs or themes, like the ever popular holiday stamps for Christmas.

The various postal authorities contend that they lose an appreciable amount on revenue to stamp counterfeiters, and to those who "wash" stamps, that is clean off the cancellation ink and then sell the stamp for reuse. I suppose there is a small clientele for counterfeit stamps, whose use would cheat the post office out of some relatively small amount of money. Over time such losses would mount up and naturally the thing to do would be to make it harder to counterfeit stamps, which would lead to the addition of more security features to stamps. However the clear trend, at least in the US has been to remove security features from stamps. At one time all stamps had to have some form of intaglio printing, and then gravure stamps appeared. Arguably gravure is an intaglio process, but its finished product is virtually indistinguishable from a similar offset image. And then many stamp issues have gone to only offset printing, which could be replicated in hundreds if not thousands of printing shops nationwide.

Stamp washing has been shown to be a lucrative business, and anyone caught washing and recycling stamps should get some time in a controlled environment, such as jail. However, here again the protest against revenue loss is hollow, as many stamps in circulation are not cancelled, and would not have to be washed to be reused. I estimate from my personal mail that about one percent of stamps are not cancelled. If there is a thirty-five billion stamp program and each stamp is worth 34 cents, then about $11billion is spent on stamps. One percent of that figure is $110 million dollars, far more than is lost in stamp washing schemes.

So what is being protected when an optical device is added to a postage stamp? I heretically suggest that the thing being protected is the revenue flow to the postal authority, which is able to sell stamps, and often high value stamps, and not ever provide any service. Except for the cost of the stamp, that is called "profit." And what is more eye-catching than a shiny reflective hologram or a stamp that changes colors depending on the viewing angle?

That said, let's look at holograms on stamps. According to the list in Linn's Stamp News[6], Austria issued the first hologram stamp on October 18, 1988. As of July 2000, at least 87 holographic stamps, envelopes and other postal stationery had been issued. An excellent pictorial discussion of hologram stamp production is contained in Scott Stamp Monthly, July 2000.[7]

But holograms and diffraction gratings are not the only optical trick available. OVI® ink has been used on postage stamps to good effect.

Naturally if the stamp has a high face value, it makes more sense to add security features to protect the stamp and its revenue stream. Such a stamp is the British ten pound Britannia stamp of 1993.[8] At least nine separate technologies and printer's tricks are used to add to the security of this stamp.

4. FUTURE NEEDS AND APPLICATIONS

What work remains to be done to further secure the place of optical features in ID and value documents like currency and postage stamps?

4.1 Greater market penetration

Many value documents do not have optical security features. Those that do not, need to be upgraded. In some cases the argument to upgrade may be that the cost of not upgrading (in lost revenue, increased illegal immigration, reduction in bond rating) is worse than the cost of upgrading the documents in question.

4.2 Increased standardization

In the standards writing field, the more that such features are raised from the "nice to have" category to the "need to have" category will help increase the use. Such efforts underway now to define a common driver's license standard and the "Minimum security standards for travel documents" are excellent areas to increase the acceptance and use of enhanced optical features.

4.3 Increased readability

Great capital is made of the ability of the human eye to discern the optical features that have been discussed in this paper. On the other hand, in many cases the difference between shadings or optical responses is too small for the eye to see. In other cases, the uniform, unblinking electronic eye is superior to the human eye that gets tired and changes optical sensitivity characteristics over time. In the travel document field, full-face readers are becoming the norm. The ability to measure several key aspects of an optically variable image would enhance the utility of such devices.

4.4 Increased memory

Holograms have the potential to store huge amounts of information. However in their use in present documents the information storage aspect has been forgotten or ignored. If there were a way to recapture this ability, then whole new opportunities for security would open up.

4.5 Hologram personalization

With the exception of the new German passport and ID card, no other country is issuing a document with a holographic portrait of the holder. While this may be easier to attain in the volume hologram system, it may require new methods of origination to enable other reflective or refractive holograms to also demonstrate this capability.

5. SPECIAL ACKNOWLEDGEMENT

Special thanks to John Hotchner, Passport Services, for providing the philatelic examples, and to Chris Larson, Office of Fraud Prevention Programs, who skillfully adds the graphics to the Power Point presentations.

6. REFERENCES

1. Bible, 1Kings 21:8 and Esther 8:8
2. D. Hunter, *Papermaking,* p. 474, Dover Publications, New York, 1978
3. W. Kranister, *The Moneymakers,* Black Bear Press, Cambridge, UK, 1989
4. M. Bloom, *The Brotherhood of Money,* BNR Press, Port Clinton, Ohio, 1983
5. Intergraf 2001 Exhibition Catalog, p85, Intergraf, Brussels, 2001
6. Linn's Stamp News website, linns.com/hologramstamplist
7. P. Martin, "An inside look at U.S. hologram stamp production," Scott Stamp Monthly, July, 2000, pp 48-49
8. T. Current, "The Album Page" newsletter, pp 4-5, November 1997